FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 6.0.1 GA

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 28, 2018

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-06-28	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.1 release, build 0102.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000D
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FortiMail VM [AWS(BYOL)]
- FortiMail VM [Azure(BYOL)]

What's New

The following table summarizes the new features and enhancements in this release.

Features	Descriptions
Disclaimer insertion action	Added disclaimer insertion action to all the action profiles, so that it can be used in the policies. Before 6.0.1 release, disclaimers can only be used at system and domain levels.

SMTP delivery preference control	Google business email service does not accept multiple destination domains per SMTP transaction, resulting in repeated delivery attempts and delayed email. To work around this Google limitation, the following CLI command has been added:
	`config system mailserver`
	`  set smtp-delivery-session-preference {domain | host}`
	`end`
	The default setting used to be host. Multiple recipient domains that resolve to the same MTA are sent to the server in the same session.
	Now the default setting is changed to domain. Multiple recipient domains that resolve to the same MTA will be sent to the server in separate sessions.

Header manipulation enhancement	Starting from 6.0.1, header manipulation supports insertion of variables.
Log retention period and log access	Added log retention period setting under Log & Report > Log Settings. Also able to log administrator's access to logs under Monitor > Log > System Event.
Logging HA mismatched checksum settings	Checksum mismatch is a common cause of HA issues. In order to find out which setting has caused the mismatch, system administrators have to manually dump the checksums on both systems and compare them one by one. This is very time-consuming. To facilitate troubleshooting, starting from 6.0.1 release, FortiMail is able to log the settings of the mismatched checksum items when the HA master and slave units are out of synchronization.
FIPS/NDcPP compliance	FortiMail 6.0.1 release is FIPS/NDcPP compliant.
AV engine upgrade	Merged FortiClient AV engine 6.0.

What's Changed

The following table summarizes the behavior changes in this release.

Features	Descriptions
TLS 1.0 support	Strong-crypto is enabled and TLS 1.0 is disabled by default in 6.0.0 release. Because some old versions of email clients (for example, MS Outlook 2007 and older) and MTAs only support TLS 1.0, they may have issues connecting to FortiMail. To fix the issue, use CLI command “config system security crypto” to disable strong-crypto and add TLS 1.0 support. For details, see FortiMail CLI Reference Starting from 6.0.1 release, TLS 1.0 is enabled by default.

Special Notices

TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiMail configurations and replace them with factory default settings.

Monitor settings for web UI

To view all objects in the web UI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

Recommended browsers on desktop computers for administration and Webmail

- Internet Explorer 11 and Edge 40, 41
- Firefox 52.7.2 ESR, 59
- Safari 10, 11
- Chrome 65

Recommended browsers on mobile devices for Webmail access

- Official Safari browser for iOS 10, 11
- Official Google Chrome browser for Android 6.0 to 8.0

FortiSandbox support

- FortiSandbox 2.3 and above

SSH connection

For security reasons, starting from 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, challenge/response should be used.

Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *System* > *Maintenance* > *Configuration*.
- After any firmware upgrade/downgrade:
  - If you are using the web UI, clear the browser cache prior to login on the FortiMail unit to ensure proper display of the web UI screens.
  - The antivirus signatures included with an image upgrade may be older than those currently available from the Fortinet FortiGuard Distribution Network (FDN). Fortinet recommends performing an immediate AV signature update as soon as possible.

Upgrade path

For any 5.x release

Any 5.x release older than 5.2.3
↓
5.2.3 (Build 436)
↓
5.2.8 (Build 467)
↓
5.3.10 (Build 643)
↓
5.4.4 (Build 714) (Required for VMware install only)
↓
6.0.1 (Build 0102)

For any 4.x release

Any 4.x release older than 4.3.6
↓
4.3.6 (Build 540)
↓
5.2.3 (Build 436)
↓
5.2.8 (Build 467)
↓
5.3.10 (Build 643)
↓
5.4.4 (Build 714) (Required for VMware install only)
↓
6.0.1 (Build 0102)

After every upgrade, verify that the build number and branch point match the image that was loaded by going to *Dashboard* > *Status* on the Web UI.

Firmware downgrade

Downgrading from 6.0.1 to 5.x or 4.x releases

Downgrading from 6.0.1 release to any 5.x or 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 6.0.1 configuration.
2. Install the older image.
3. In the CLI, enter `execute factoryreset` to reset the FortiMail unit to factory defaults.
4. Configure the device IP address and other network settings.
5. Reload the backup configuration if needed.

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Antispam/Antivirus/Content

Bug ID	Description
493838	URIs are not submitted to FortiSandbox in some cases.
495608	Unable to release or view System Quarantine search results.
491213	FortiMail should not send URIs in the HTML title tags to FortiSandbox.

System

Bug ID	Description
495162	When all IBE secure questions are disabled by the administrator, three questions are still displayed to the IBE email users.
498174	LDAP alias expansion should not be case sensitive.
498002	Some sensitive information may be exposed in the IBE trace log under certain conditions.
498028	Fixed a security vulnerability identified by internal code review (FG-IR-17-126).

Admin GUI/Webmail

Bug ID	Description
497787	System time on the Dashboard is not accurate for some time zones.
482891	IP address and port number combination is not accepted for FDS override IP address under System > FortiGuard > Antivirus.

Known Issues

The following table lists some minor known issues. .

Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

Image Checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool